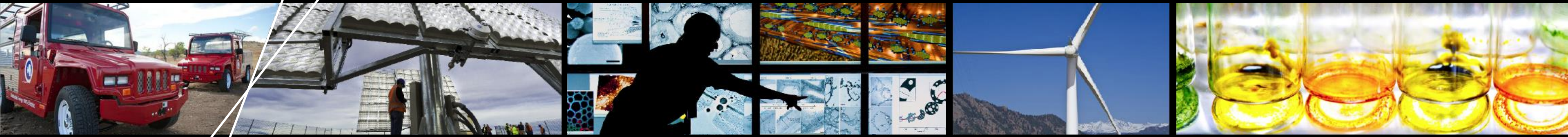
NATIONAL RENEWABLE ENERGY LABORATORY

Cyber-Physical Systems Security & Resilience Center



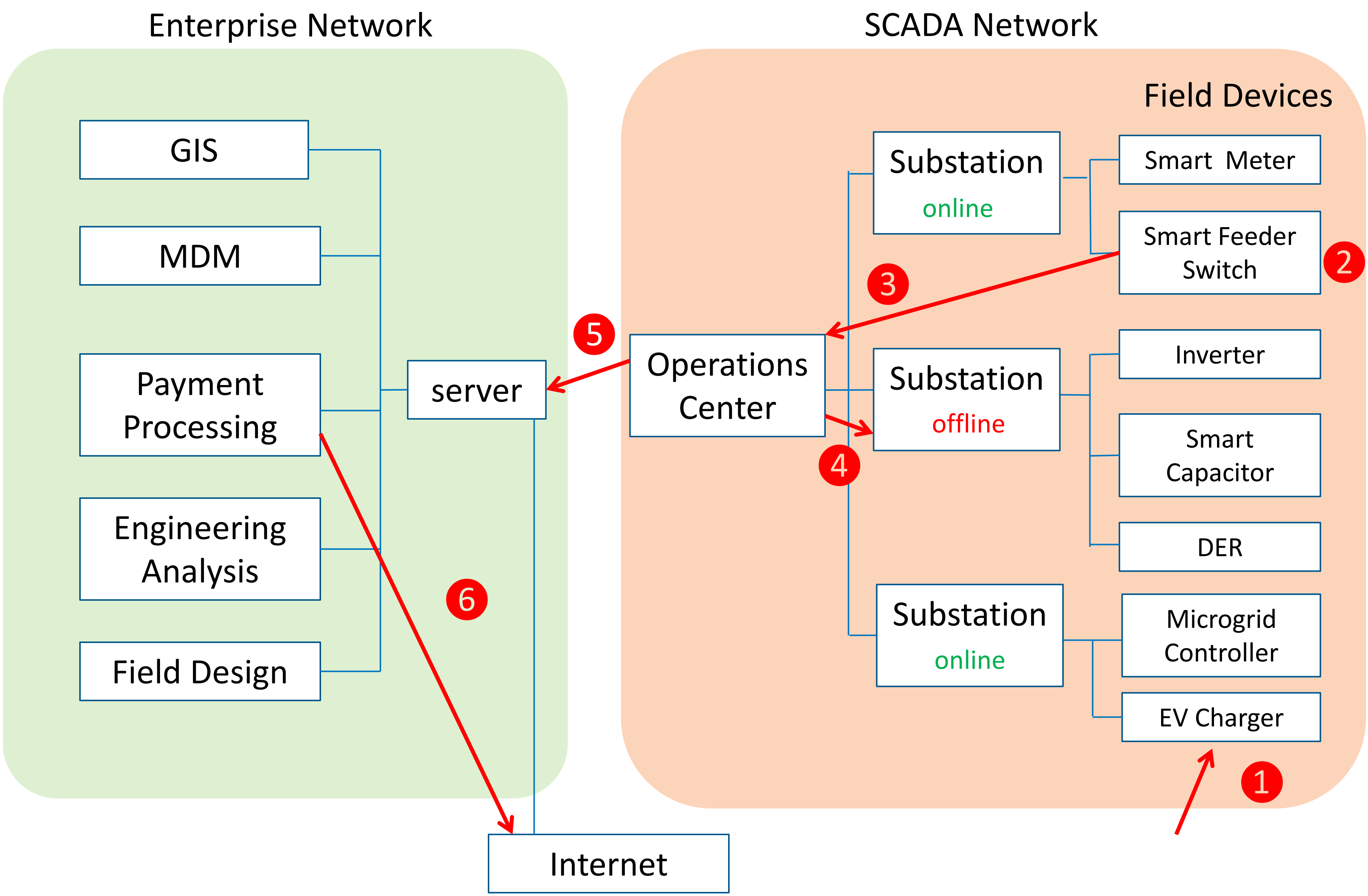
Insecure Field Devices on the Smart Grid: Cyber Risks, Damage Potential, and Practical Solutions

Maurice Martin

25 Feb 2016

NREL is a national laboratory of the U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, operated by the Alliance for Sustainable Energy, LLC.

Distribution utility attack



Today's Webinar

Energy Systems Integration

1. Dangers arising from insecure smart grid field devices

2. Resources available to address the issue (and why they may go unused)

3. Technologies for identifying vulnerabilities in individual devices

4. NREL Research

National Renewable Energy Lab

Energy Systems Integration

Our Vision …

Secure the prosperity of our nation.

Our Mission …

Apply innovative technology, business processes, and policy to produce tangible improvements in the cyber-physical security posture of critical infrastructure and verticals most important to our economy.

Cyber-Physical Systems Security & Resilience Center (CPSSR)

Energy Systems Integration

- **Dr. Erfan Ibrahim, Center Director**
- PhD Nuclear Engineering, UC Berkeley
- Lawrence Livermore National Lab, Pacific Bell, EPRI, Bit Bazaar
- Chief liaison to the Office of Electricity Delivery and Energy Reliability. GMLC Cybersecurity and Resilience team member
- Identifies security requirements, evaluates cybersecurity standards, test cybersecurity controls

- **Tami Reynolds, Business Development Support & Project Leader**
- BS Business-Marketing, Metropolitan State University of Denver
- Business Development for NREL's Energy Systems Integration
- Leads projects through development, planning, contracting, equipment procurement, and technology transfer

Cyber-Physical Systems Security & Resilience Center (CPSSR)

Energy Systems Integration

- **Michael Ingram, Group Manager and Business Area Lead**
- MS Engineering/Industrial Management, University of Tennessee - Chattanooga
- Tennessee Valley Authority, operations specialist and senior advisor
- Manages research program, develops empirically-based security architectures and resilience best practices

- **Ivonne Peña, Policy Area Lead**
- PhD Engineering and Public Policy, Carnegie Mellon University
  PhD Engineering, Technical University of Lisbon, Portugal
- Westeva co-lead for business and analytics, United Nations
- Analyzes and develops policy mechanisms to incentivize cyber security improvements

- **Maurice Martin, Technology Area Lead**
- MS Systems Science, Louisiana State University
- National Rural Electric Cooperative Association, cyber security research lead
- Manages research projects, provides system-level analysis for cybersecurity initiatives, serves as liaison to utility industry associations

Cyber-Physical Systems Security & Resilience Center (CPSSR)

Energy Systems Integration

- **Brian Miller, Senior Engineer**
- MS Electrical Engineering, University of Tennessee – Knoxville
  MS Military Operations, Air Command and Staff College
- U.S. Air Force, design engineer and project manager
- Implements power system projects; conducts site assessments, modeling, and analysis of complex systems (including microgrids)

- **Randolph Hunsberger, Senior Engineer**
- MS Building Systems, University of Colorado - Boulder
- Consultant for renewable energy projects around the U.S.
- Operates CPSSR's Secure Distribution Grid Management Testbed, manages and maintains network resources for cybersecurity use cases and penetration tests

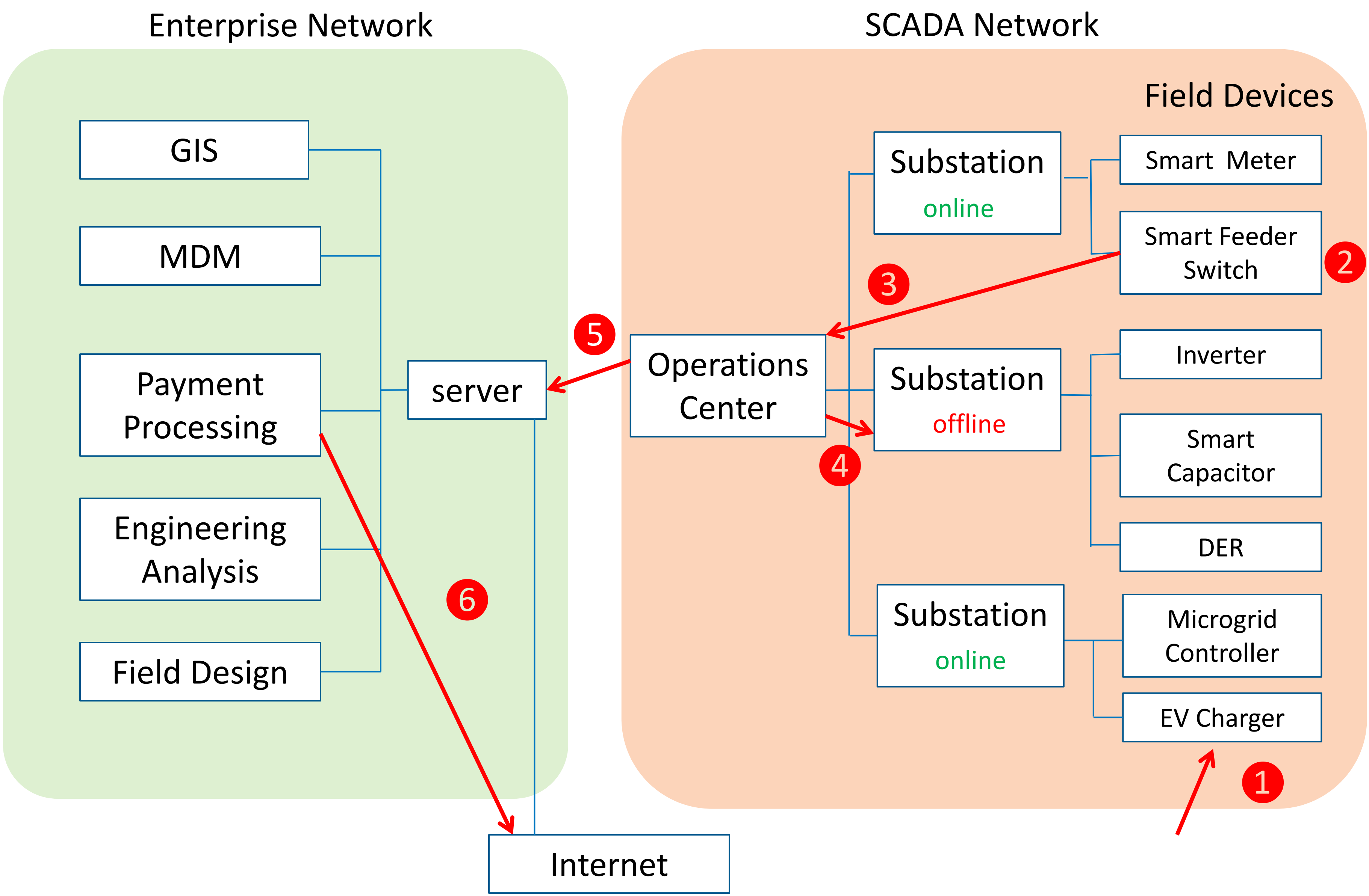
Smart Grid Field Devices

- Smart meters
- Smart feeder switches
- Inverters
- Smart capacitors
- Distributed Energy Resources (DERs)
- Microgrid controllers

Part 1
Dangers arising from insecure smart grid field devices

Distribution utility attack

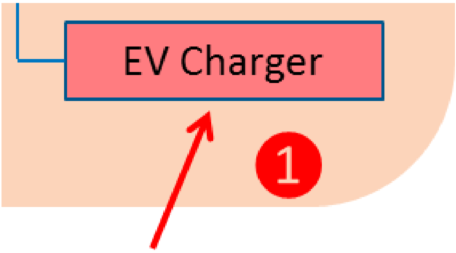
Energy Systems Integration



1) Compromise a field device

Where are field devices?

- **Customer homes**
  - smart meters
- **Utility poles**
  - smart switches
- **Public spaces**
- **Substations**
  - microgrid controllers
  - Inverters



THE RISE OF COPPER THEFT
& ITS THREAT TO U.S. CRITICAL INFRASTRUCTURE

"Copper thieves are threatening U.S. critical infrastructure…and present a risk to both public safety and national security."
– Federal Bureau of Investigation

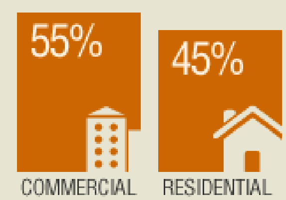
Since August 2009, metal thefts have steadily increased across the nation, driven by rising prices for base metals... especially copper.

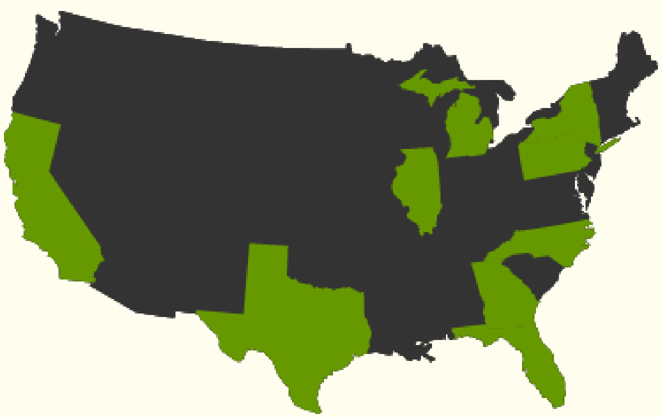
Whether the theft is an expensive personal irritant, like finding your catalytic converter has been stolen, or one that threatens public safety, as when the theft of copper wiring blacked out runway approach lights at the Modesto, CA, regional airport—metal thefts are increasing in frequency and severity.

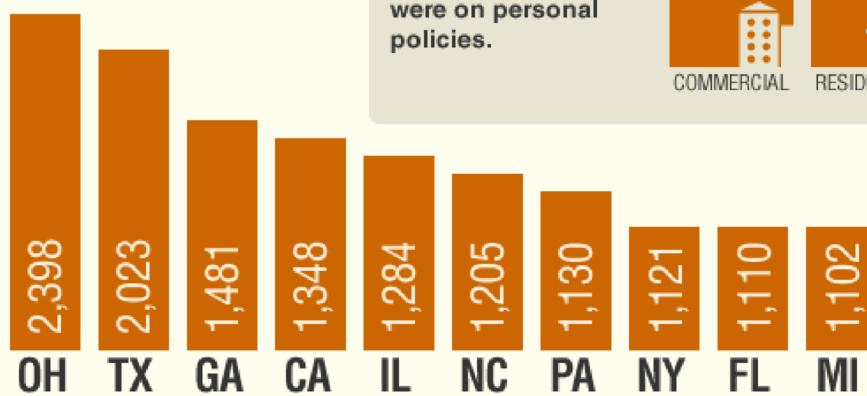
WHERE IS COPPER BEING STOLEN FROM?

Over 25,000 claims for the theft of copper, bronze, brass, or aluminum were submitted to ISO ClaimSearch from 2009 to 2011. Of these, **96% concerned copper theft.**

55% of the claims were on commercial policies, while 45% were on personal policies.





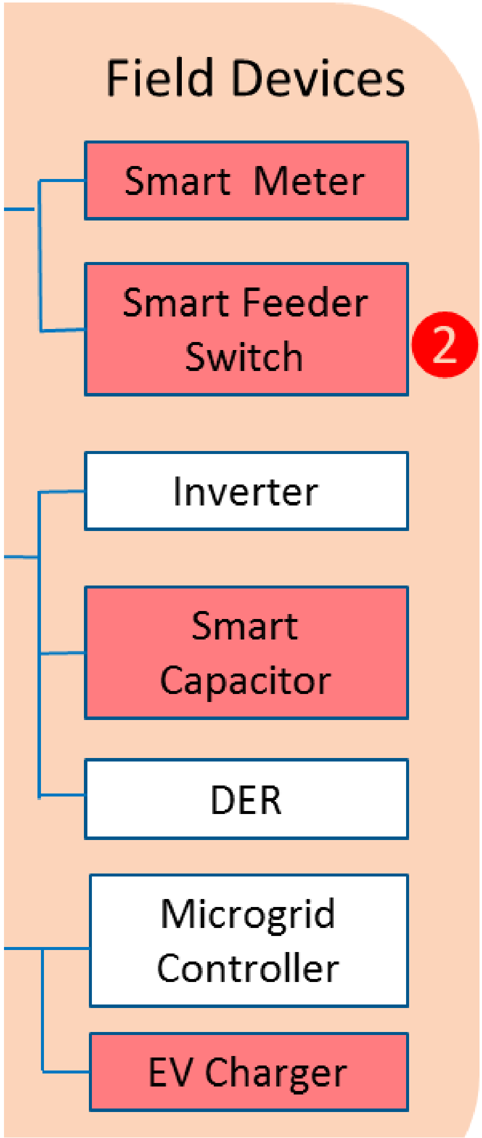


Data: The National Insurance Crime Bureau

Graphic: Super | Circuits

Increasingly, field devices have embedded operating systems

- Itron and Cisco have embraced Linux
- Having a full operating system to work with gives hackers more tools



Demonstrated in a lab

Demonstrated in a field: 2012

Energy Systems Integration

Project Carna

- **Academic researches created a botnet**
- **Devices with embedded operating systems**
- **420,000 devices**
- **Used to gather data**
  - Services
  - IPv4 addresses
- **Weak or absent passwords**

Demonstrated in a field: 2014

Energy Systems Integration

proofpoint

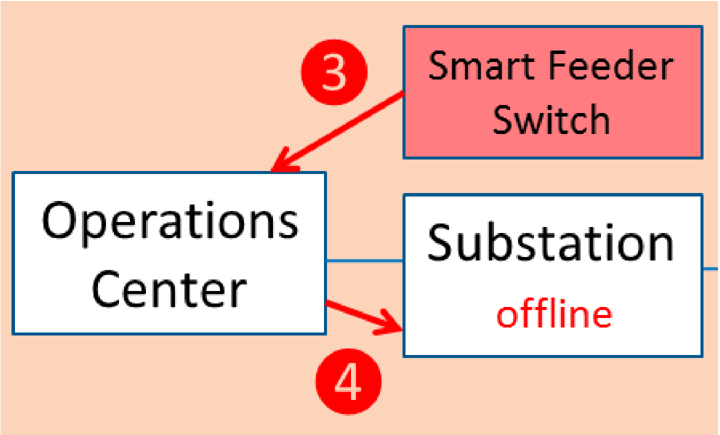
- **Discovered first IoT botnet**
- **100,000 consumer devices**
- **750,000 malicious emails**
- **Included:**
  - Home routers
  - multi-media centers
  - televisions
  - at least one refrigerator

The Smart Grid is one instance of the "Internet of Things."

same challenges

Attackers shutting off part of the grid.

- Until recently, no instance of this. However…



First power outage due to hacking

(At least, the first we know of…)

23 Dec 2015

4pm

- Two electric utilties:
  - Prykarpattyaoblenergo
  - Kyivoblenergo
- 80,000 customers
- All power restored within 3.5 hours

What did the hackers do?

Energy Systems Integration

1. Opened circuit breakers in a number of substations, shutting off power.

2. Locked up the screens of dispatchers and operators, slowing response time.

3. Wiped data from the SCADA system.

4. Launched a telephone denial of service (TDOS) attack to disrupt communication/slow recovery.

How did the hackers do it?

Energy Systems Integration

Action	Theory	Not known
Gained access to the SCADA system	Malware	Which malware? Possibly… • BlackEnergy Also: Delivery mode
Shut off circuit breakers	With SCADA access, hackers were able to manually open circuit breakers	Everything
Locked up dispatcher's computer screens/wiped SCADA data	Malware	Which malware? Possibly… • KillDisk
Telephone Denial of Service attack	None	Country of origin for incoming calls

Could it happen in the U.S.?

Not to scale

BlackEnergy

BlackEnergy

Less automation

More automation

Gen. Michael Hayden

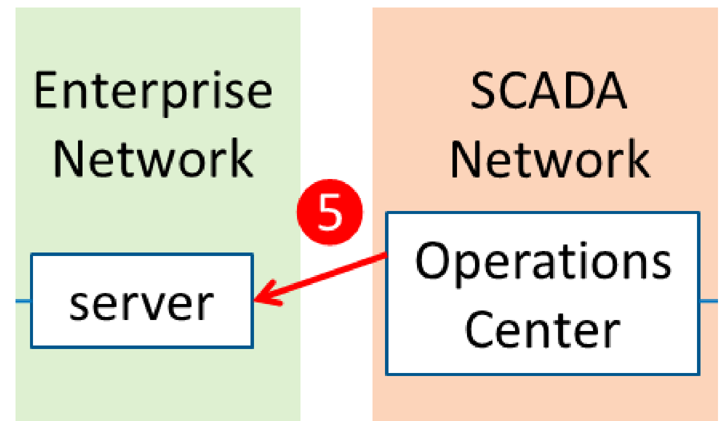
Former NSA director
Former CIA chief

What happened in Ukraine is a harbinger for the kinds of cyberthreats the US faces, possibly from rival nations such as Russia and North Korea…

(paraphrased)
Christian Science Monitor
12 Jan 2016

5) Move from SCADA network to enterprise network

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

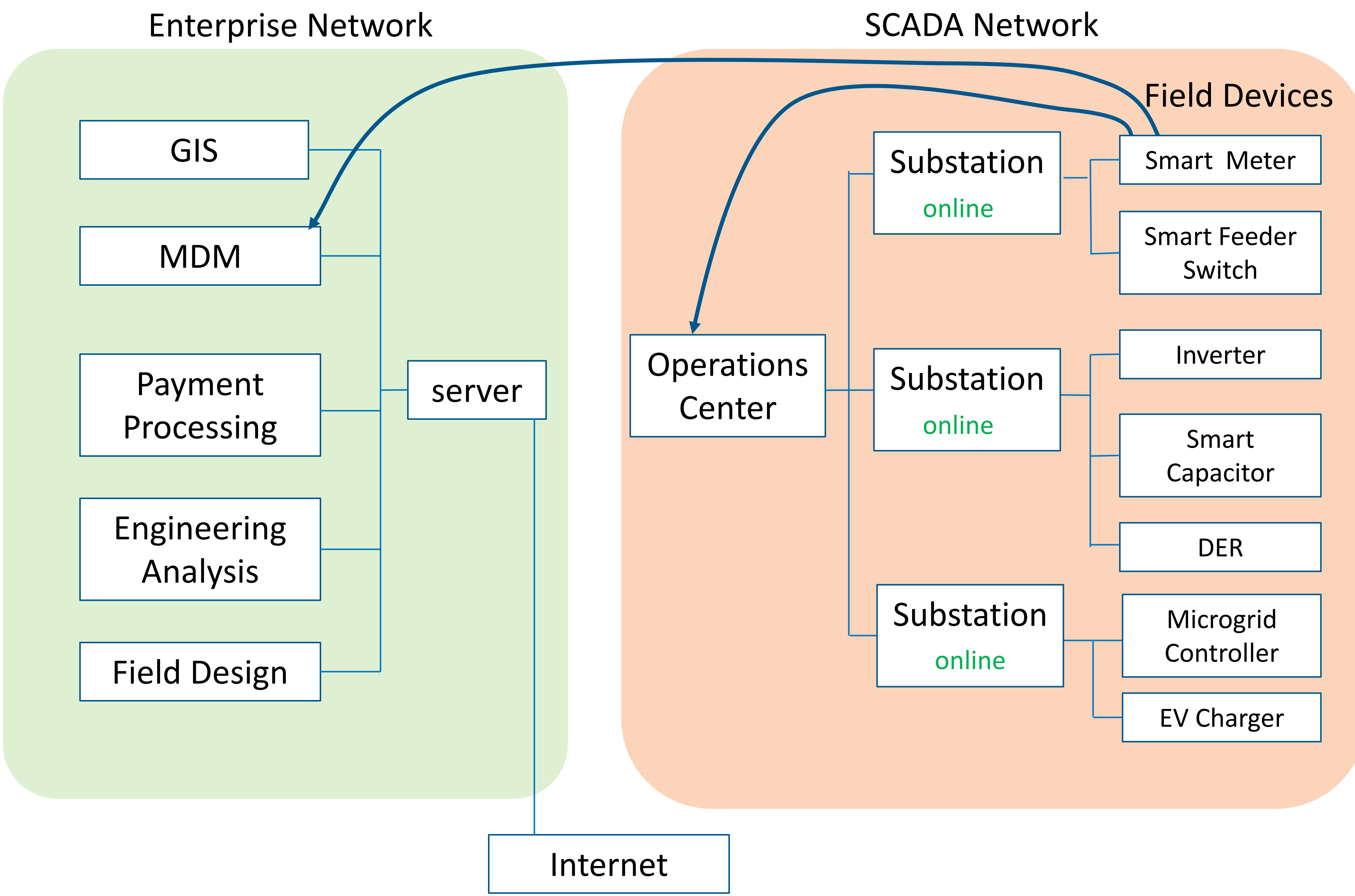


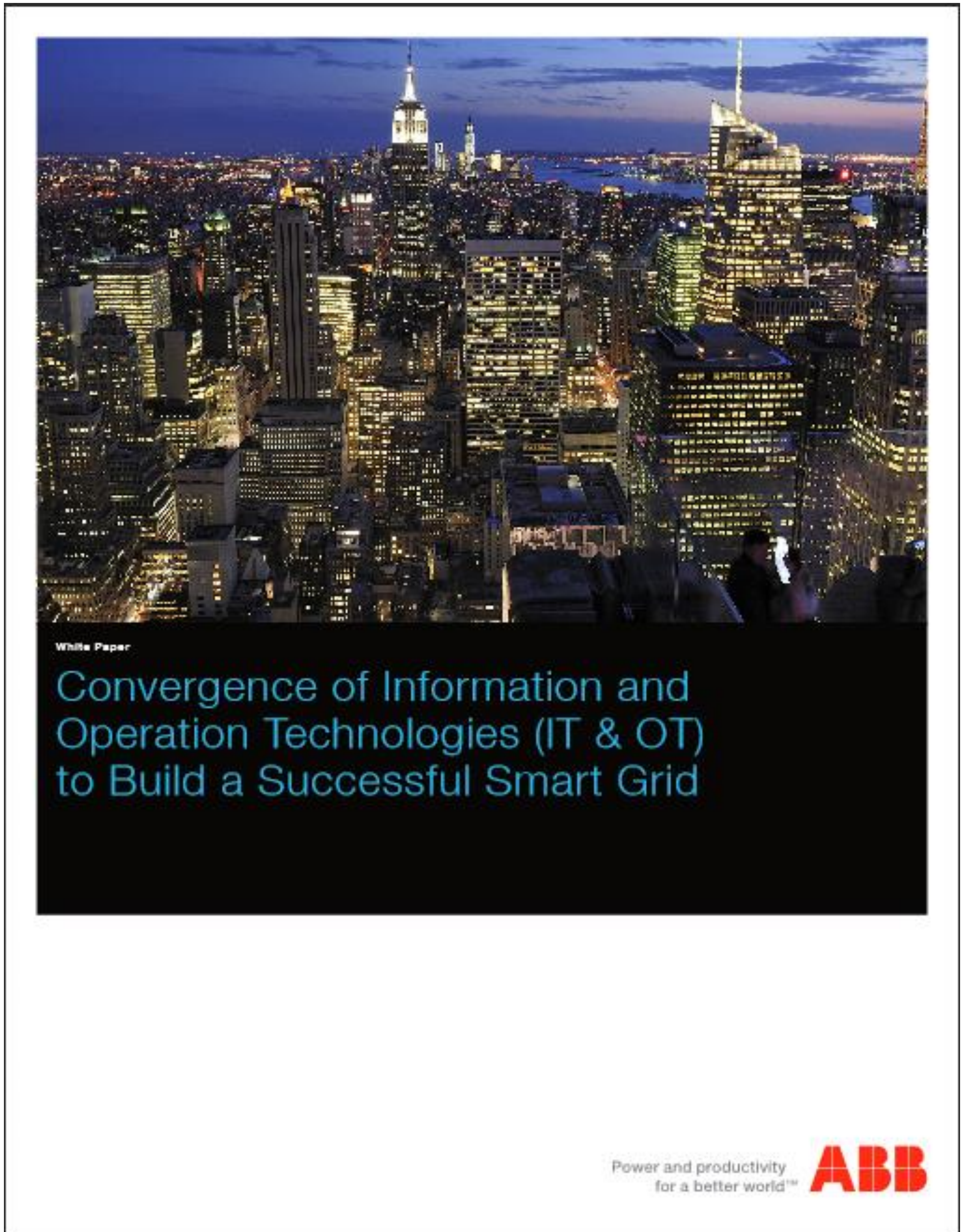
ICS-CERT says: Air gap your SCADA networks!

But do we?

Value of data (particularly meter data)

Energy Systems Integration




White Paper

Convergence of Information and Operation Technologies (IT & OT) to Build a Successful Smart Grid

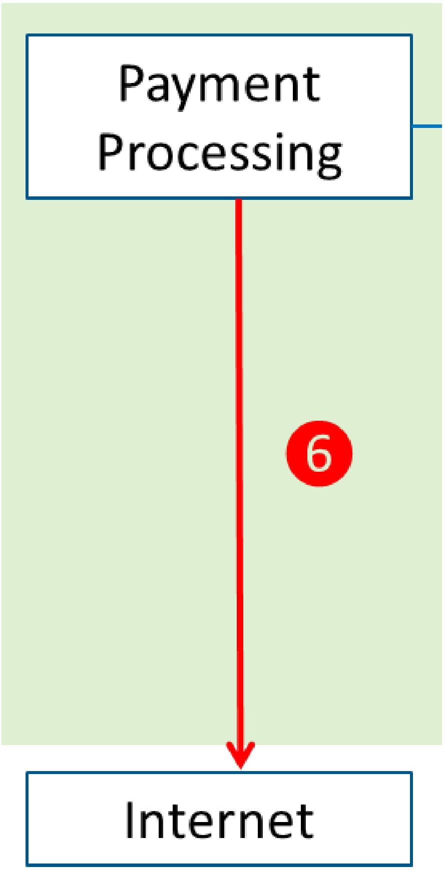
Power and productivity for a better world™

ABB

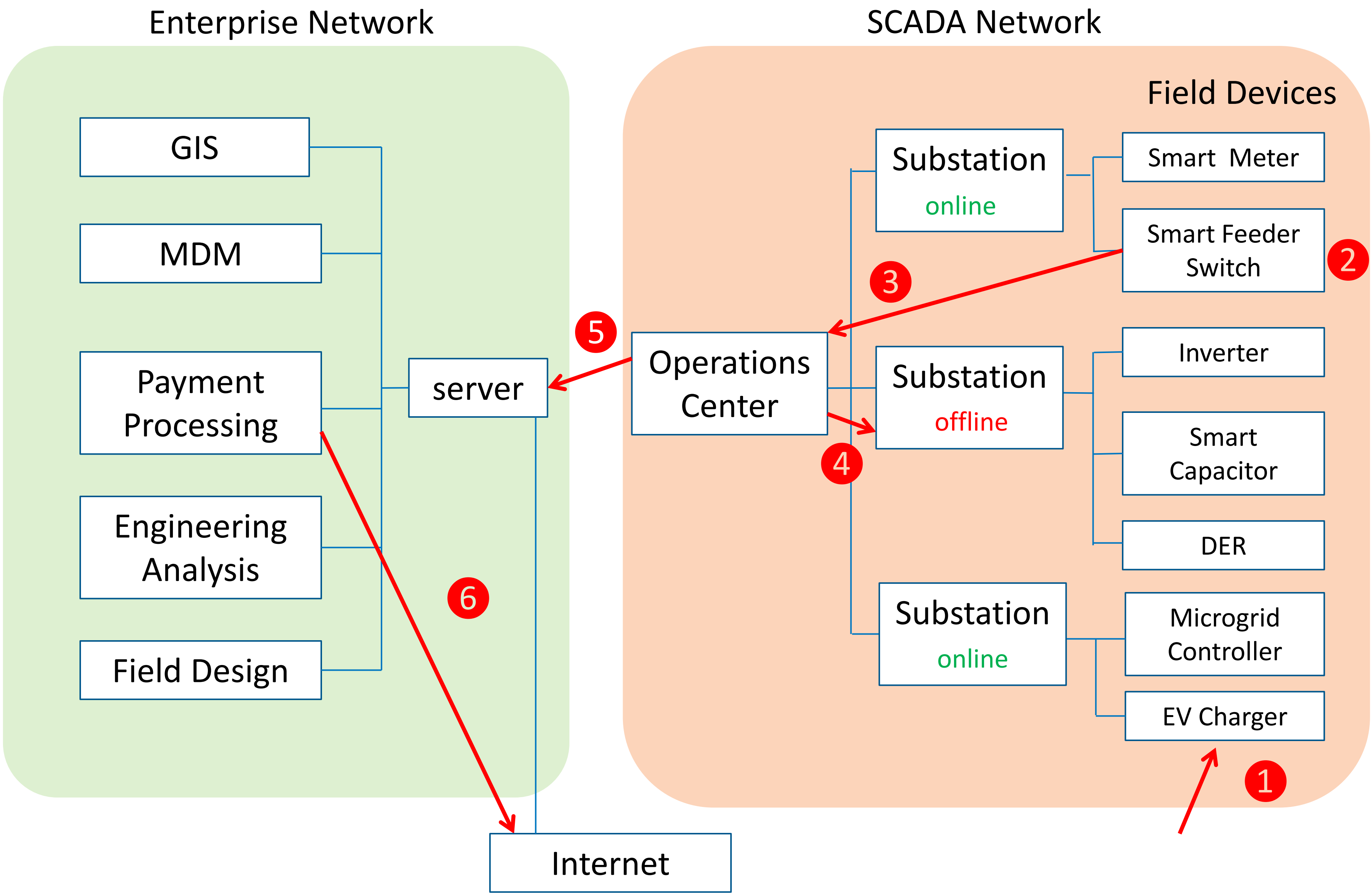
“The Integration of IT and OT is vital to a successful implementation of new technologies under the Smart Grid umbrella”

6) Exfiltrate sensitive data

Energy Systems Integration



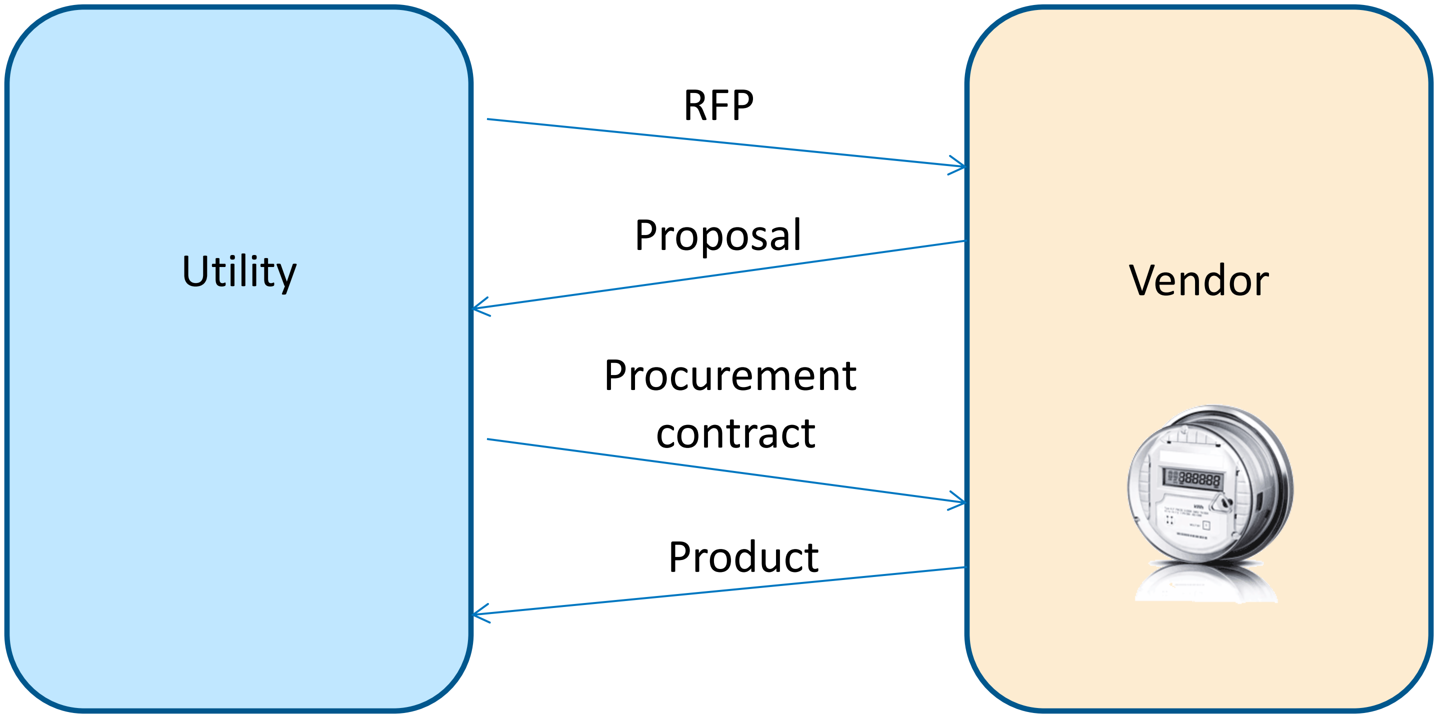
Distribution utility attack



Part 2
Resources available to address the issue
(and why they may go unused)

Procurement process

Energy Systems Integration



RFP phase

Energy Systems Integration

Security Questions for Smart Grid Vendors

NRECA has created a set of questions for utilities to submit with RFPs.

Attachment

Security Questions

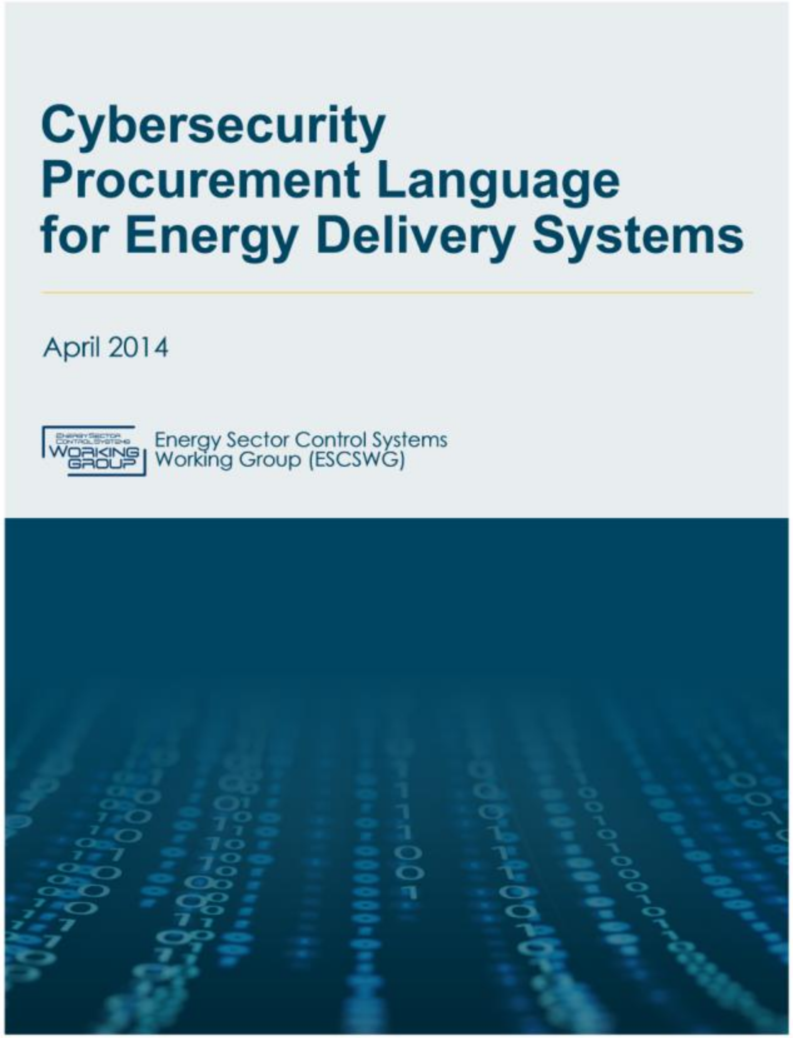
#	Description	Supplier Brief Response
	INSTRUCTIONS: The items listed below are paraphrased from the NISTIR 7628 Volume 1, which we understand to be in draft form. *These are not requirements.* We would like to learn more about the security characteristics of your product that are provided now or will be provided in the future. Please answer the questions clearly "yes" or "no," and if the proposed system is capable of accomplishing the security characteristic, please briefly describe how. If your system or product includes any security characteristics above and beyond the listed items, such as any additional considerations or enhancements as described in the NISTIR 7628, please describe those as well. *Note: the term "system" shall mean software, hardware, etc. that may exist at the head-end and/or equipment that is located remotely within the electric distribution grid.*	
1	**Reference: SG.AC-4 Access Enforcement.** Can the proposed system enforce assigned authorizations for controlling access to the Smart Grid information system in accordance with organization-defined policy? If so, please briefly describe how this is accomplished.	
2	**Reference: SG.AC-5 Information Flow Enforcement.** Does the proposed system enforce assigned authorizations for controlling the flow of information within the Smart Grid information system and between interconnected Smart Grid information systems in accordance with applicable policy? If so, please briefly describe how this is accomplished.	
3	**Reference: SG.AC-8 Unsuccessful Login Attempts.** Can the proposed system enforce a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period? If so, briefly describe how this is accomplished.	
4	**Reference: SG.AC-9 Smart Grid Information System Use Notification.** Does the proposed system display an approved system use notification message or banner before granting access to the Smart Grid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance? If so, briefly describe how this is accomplished.	

Procurement phase

Energy Systems Integration

Cybersecurity
Procurement Language
for Energy Delivery Systems

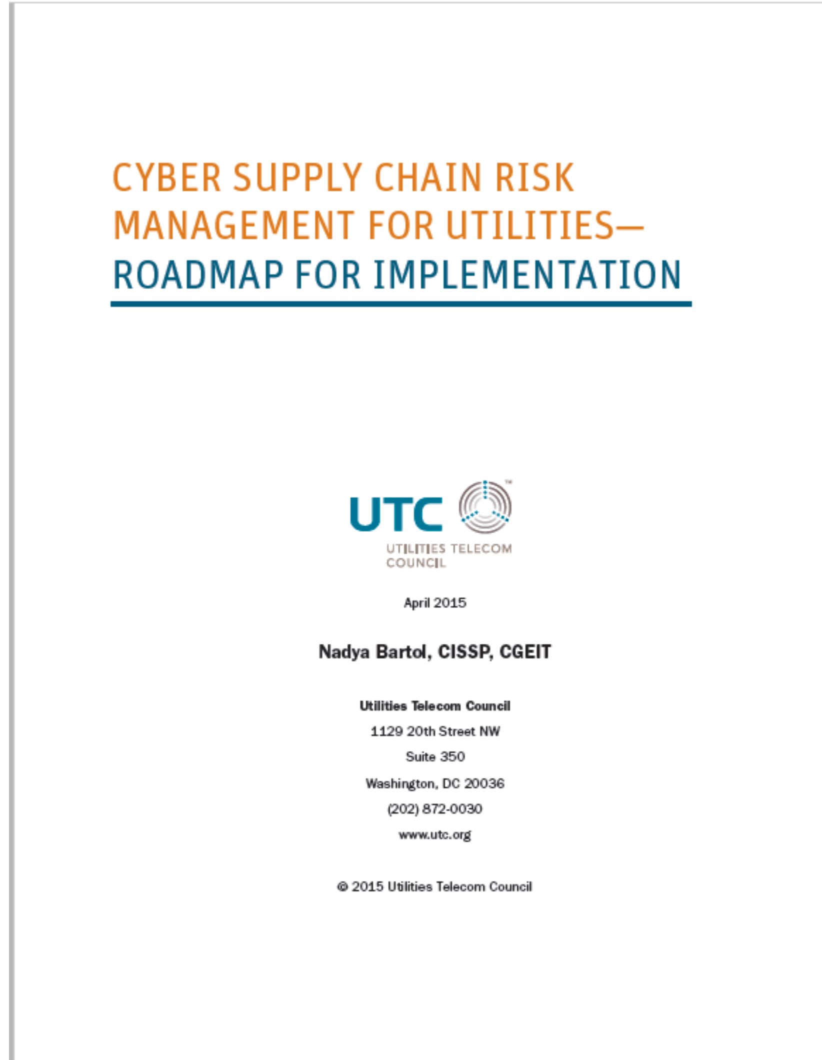
DOE funded document that provides sample language for inclusion in contracts.



Supplier relationships

Cyber Supply Chain Risk Management for Utilities—Roadmap for Implementation

UTC created this document defining 10 practices for managing supplier relationships.



CYBER SUPPLY CHAIN RISK MANAGEMENT FOR UTILITIES—ROADMAP FOR IMPLEMENTATION

UTC
UTILITIES TELECOM COUNCIL

April 2015

Nadya Bartol, CISSP, CGEIT

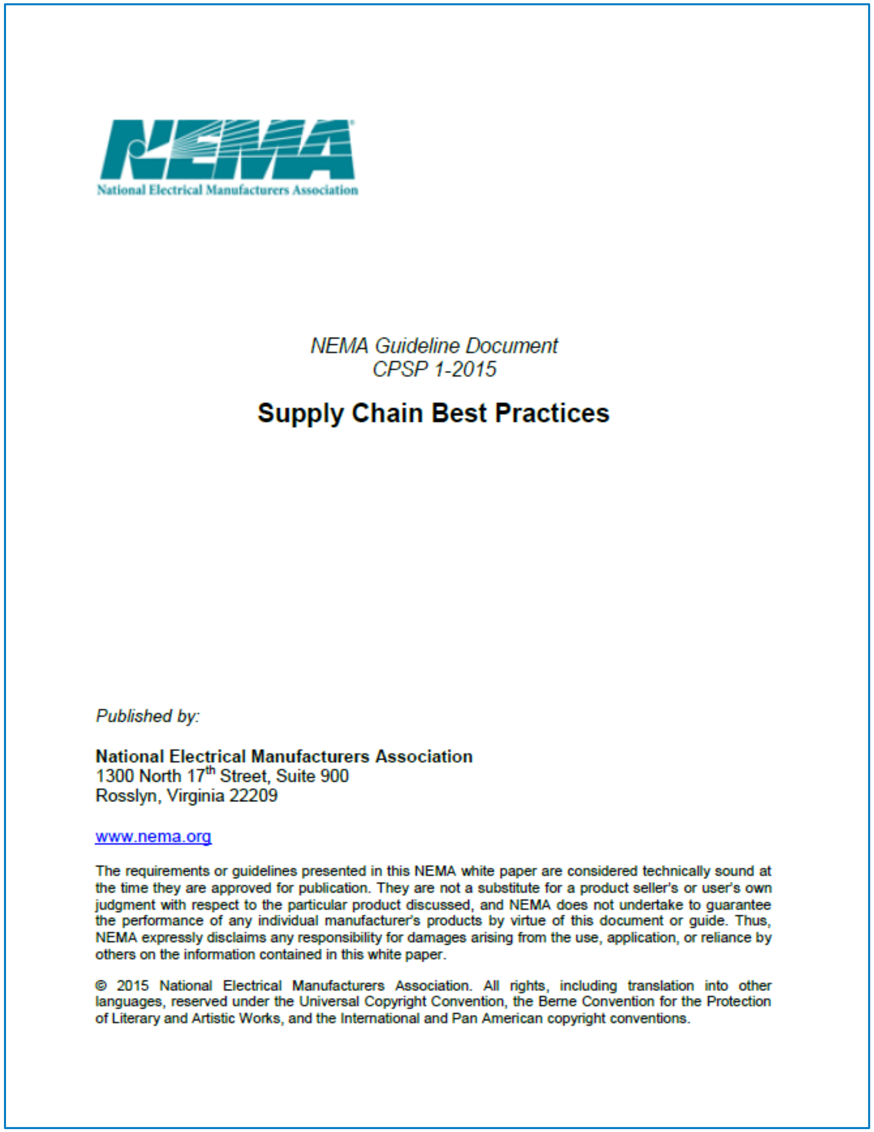
Utilities Telecom Council
1129 20th Street NW
Suite 350
Washington, DC 20036
(202) 872-0030
www.utc.org

© 2015 Utilities Telecom Council

For vendors

Supply Chain Best Practices

National Electrical Manufacturers Association recommendations on best practices for product development.



National Electrical Manufacturers Association

NEMA Guideline Document
CPSP 1-2015

Supply Chain Best Practices

Published by:

National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

www.nema.org

The requirements or guidelines presented in this NEMA white paper are considered technically sound at the time they are approved for publication. They are not a substitute for a product seller's or user's own judgment with respect to the particular product discussed, and NEMA does not undertake to guarantee the performance of any individual manufacturer's products by virtue of this document or guide. Thus, NEMA expressly disclaims any responsibility for damages arising from the use, application, or reliance by others on the information contained in this white paper.

© 2015 National Electrical Manufacturers Association. All rights, including translation into other languages, reserved under the Universal Copyright Convention, the Berne Convention for the Protection of Literary and Artistic Works, and the International and Pan American copyright conventions.

Focus: securing the enterprise network

1. **Attacks on the enterprise network have been increasing.**
   - Crypto-ransomware attacks rose 4000% in 2014.
   - Ransomware attacks rose 165% in Q1 2015.

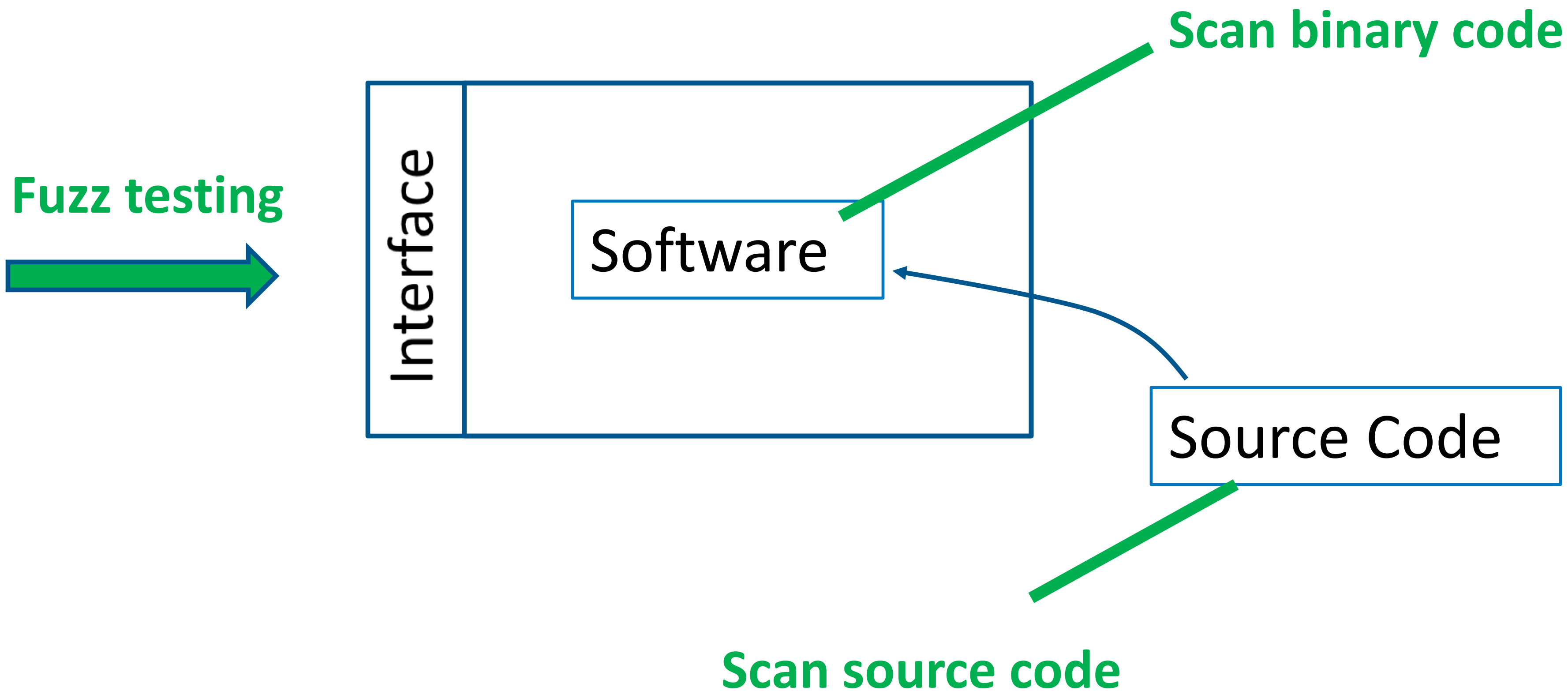
2. **Well-publicized theft of sensitive data in the retail sector.**
   - Distribution utilities face same challenge of protecting customer data.

3. **Vendors focus on enterprise network.**

Part 3
Technologies for identifying vulnerabilities in individual devices

Testing individual field devices

Verifies the final product, independent of the supply chain



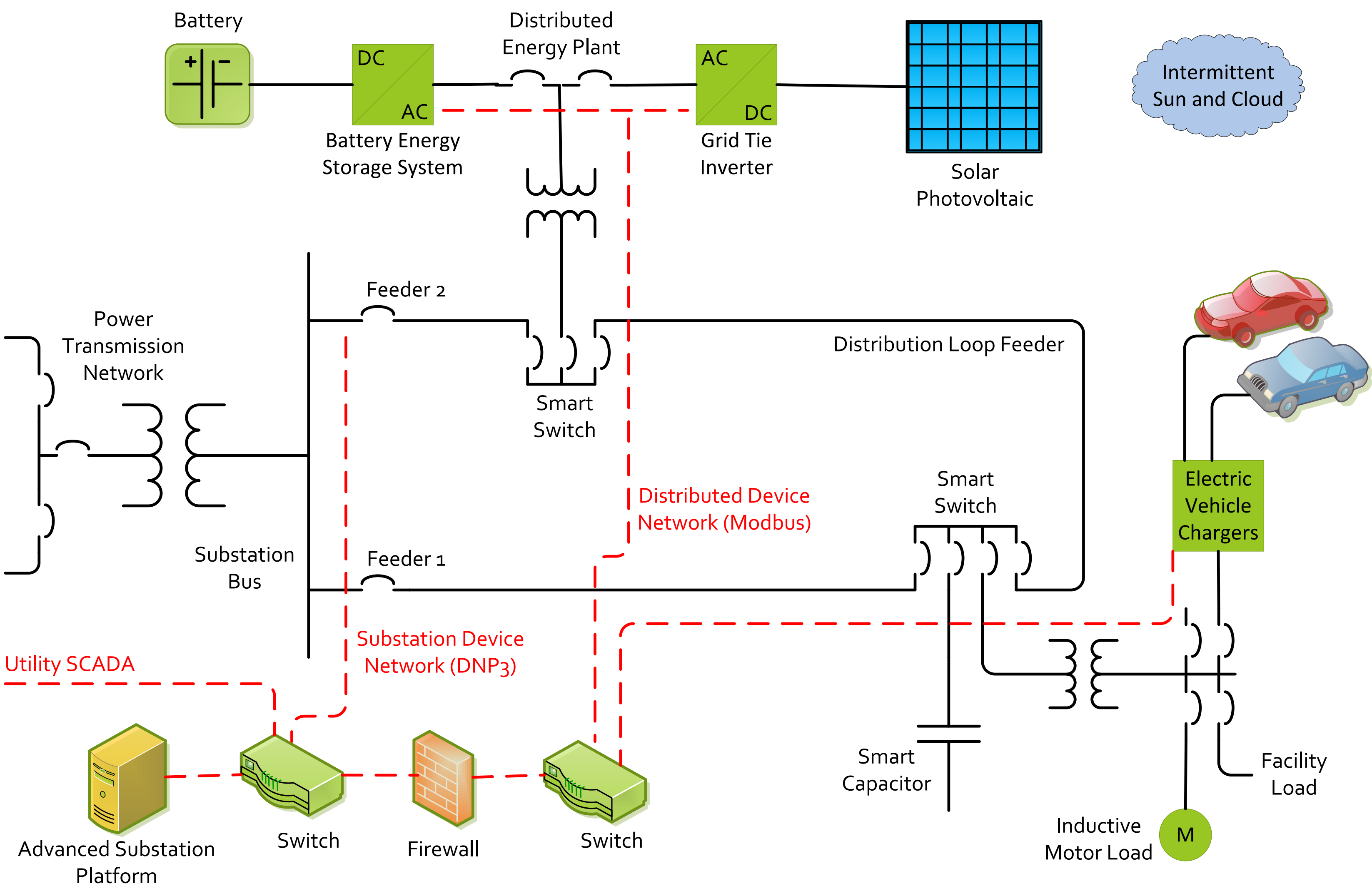
Part 4
NREL Research
(past and future)

A different approach to securing the grid

- Rather than focus on individual devices, use a systems approach
- Use only commercially available products
- DON'T lean on encryption

Communication needs

Energy Systems Integration



The testbed is a significant NREL asset.

Open Systems Interconnection (OSI) Model

Breaks the communication functions of a computing system into seven layers

	Layer	Examples
7	Application	Skype, Facebook, Youtube, Windows File Sharing, FileZilla
6	Presentation	CSS, GIF, HTML, XML, JSON
5	Session	PAP, RPC, TLS,FTP, HTTP, SMTP, SSH, Telnet
4	Transport	TCP, UDP
3	Network	AppleTalk, ICMP, IPsec, IPv4, IPv6
2	Data Link	IEEE 802.2, L2TP, LLDP, MAC, PPP
1	Physical	DOCSIS, DSL, Ethernet physical layer, ISDN, USB

GridWise® Architecture Council (GWAC) Stack

Define "degrees of interoperation necessary to enable various interactions and transactions on the Smart Grid"

	Layer	Examples
8	Economic/Regulatory Policy	Political and economic objectives as embodied in policy and regulations
7	Business Objectives	Strategic and tactical objectives shared between businesses
6	Business Procedures	Alignment between operational business processes and procedures
5	Business Context	Awareness of the business knowledge related to a specific interaction
4	Semantic Understanding	Understanding of the concepts contained in the message data structures
3	Syntactic Interoperability	Understanding of data structure in messages exchanged between systems
2	Network Interoperability	Mechanism to exchange messages between multiple systems across a variety of networks
1	Basic Connectivity	Mechanism to establish physical and logical connections between systems

9-Layer Test: Securing DGM

- Collected relevant use cases for Distribution Grid Management from the NIST Interoperability Knowledge Base (IKB)

- Collected relevant failure scenarios for Distribution Grid Management from the DoE funded NESCOR Project

- Distilled the security requirements from the use cases for the logical layers in the various environments

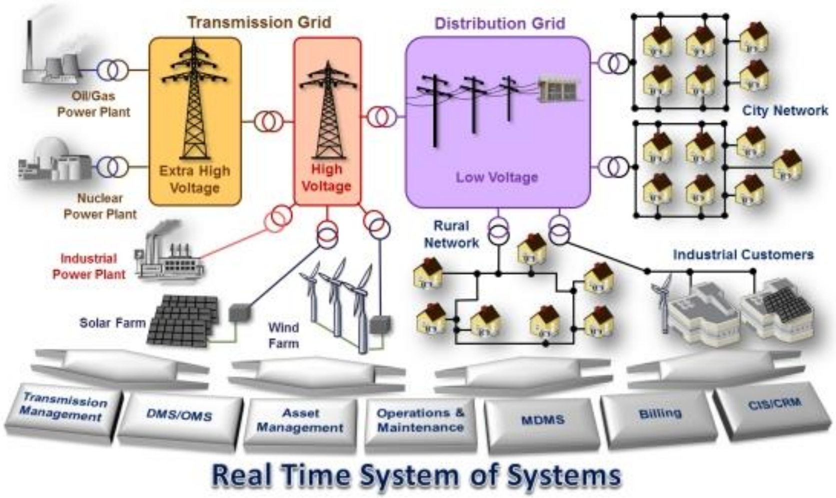
- Distilled the resilience best practices from the failure scenarios

44

Use Cases

Develop 5 use cases utilizing Distribution Grid Management application:

- Auto sectionalizing and Restoration (ASR)
- Volt-Var Optimization (VVAR)
- Demand Response with EV Charging (DR)
- PV Smoothing with Storage
- Frequency Regulation with Storage

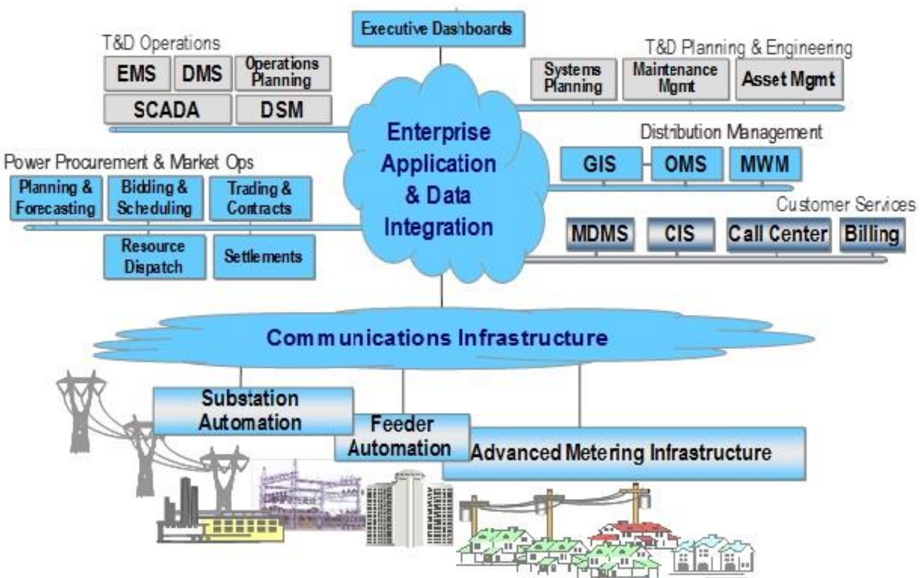


DGM Testbed

Energy Systems Integration

Built the distribution grid management (DGM) test bed with

- DMS,
- enterprise SCADA,
- substation automation platform,
- intelligent electronic devices
  - RTUs
  - PLCs
  - field sensors
- electric storage
- electric vehicles
- capacitor banks
- smart switches



Categories of Solutions Used

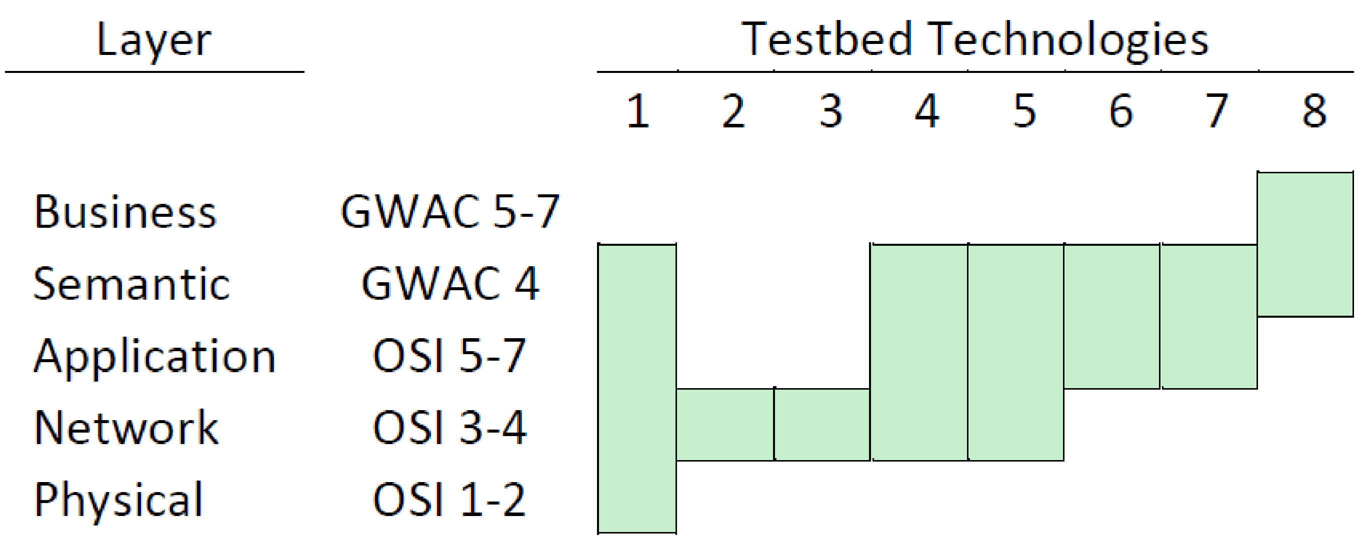
- Data diode at hardware layer
- Network and file filter at hardware layer
- Transport layer access control
- Operational situational awareness
- Malware protection for web, email and file
- Business process security

Solution: 9-Layer Security

Energy Systems Integration

The layered approach provides security at all 9 logical layers of a typical information system (7-layer OSI model + 2 upper layers of Gridwise Architecture Council Stack).

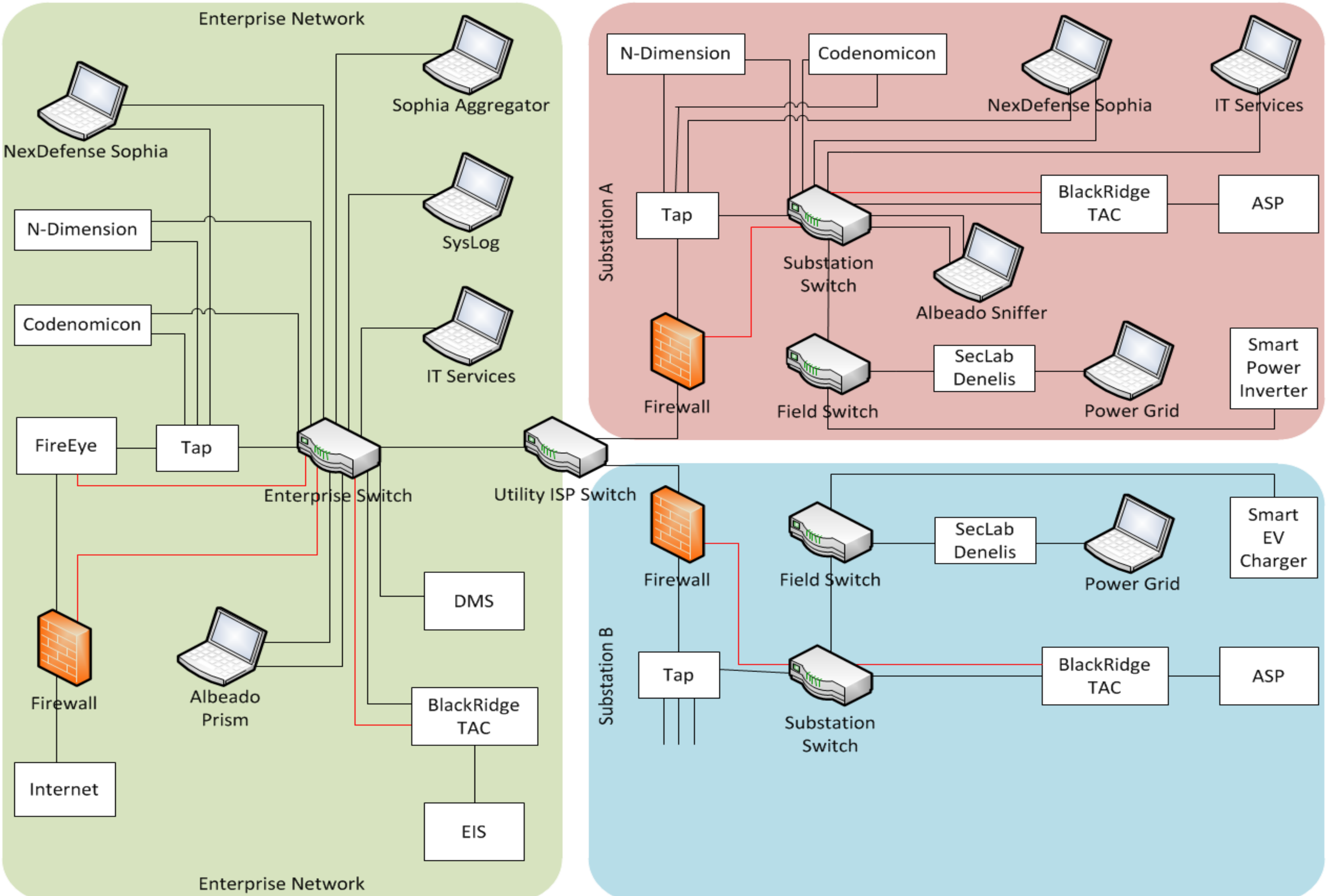
Coverage of the 8 vendor products against the 9 layers is shown schematically below.



Cybersecurity Technology Vendors

Product	Layer(s)	Technology
1. SecLab Denelis	Physical + semantic	Data filter + data diode
2. Blackridge TAC	Network	IP and TCP layer protection with authentication
3. Cisco Firewall + Cisco Switches w access control lists	Network	Stateful inspection
4. FireEye	Network + semantic	Filtering network, email, and files
5. NexDefense Sophia	Network + semantic	Anomaly detection
6. N-Dimension N-Sentinel	Application + semantic	Cloud-based continuous threat monitoring
7. Synopsys AbuseSA Intrusion Detection for SCADA	Application + semantic	Cloud-based continuous threat monitoring
8. Albeado PRISM	Business process + semantic	Business process security

Testbed



Enterprise Network
NexDefense Sophia
Sophia Aggregator
SysLog
IT Services
N-Dimension
Codenomicon
FireEye
Tap
Enterprise Switch
Utility ISP Switch
Firewall
Albeado Prism
DMS
BlackRidge TAC
EIS
Internet
Enterprise Network
Substation A
N-Dimension
Codenomicon
NexDefense Sophia
IT Services
Tap
Substation Switch
BlackRidge TAC
ASP
Albeado Sniffer
Firewall
Field Switch
SecLab Denelis
Power Grid
Smart Power Inverter
Substation B
Firewall
Field Switch
SecLab Denelis
Power Grid
Smart EV Charger
Tap
Substation Switch
BlackRidge TAC
ASP

Distribution Grid Management (DGM) Testbed

- Applied the cybersecurity controls and resilience mechanisms using the technologies from the selected vendors
- Ran the DGM use cases on the test bed; performed vulnerability/penetration testing to identify residual risk
- Confidentially recommended additional security controls to the vendors involved in the project to secure DGM
- Prepared report documenting the results of the project

Results

- Demonstrated the value of layered security in protecting against a variety of threat vectors (internal and external to an organization);
- Proved “off the shelf” cybersecurity technologies today—combined with sound cybersecurity management principles—can successfully protect organizations from these threats;
- Delivered a new R&D capability within NREL to help protect utility infrastructure, and as well as a valuable tool for DOE to secure their national lab infrastructure.

Next steps

Energy Systems Integration

- Bring data from all eight vendors into one dashboard
- Make the testbed rapidly reconfigurable
- Improve remote access capabilities
- Demonstrate what can be achieved by hacking field devices, and test defenses against such attacks.

Conclusions

- **Need for better field device security?**
  - <u>Absolutely!</u>

- **However, a systems approach to cyber security can protect against a wide variety of attacks, including those arising from insecure field devices.**

55

Contact

Energy Systems Integration

- **Maurice Martin**
  CPSS&R Technology Lead
  maurice.martin@nrel.gov

- **Tami Reynolds**
  CPSS&R Business Development Support & Project Leader
  tami.reynolds@nrel.gov